System and Method for Authorization of Access to A Resource

(A-70554/RMA)

WE CLAIM:

1. A computer program product for use in conjunction with a computer system having a server and a client, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism, comprising: a program module that directs the computer system and/or components thereof including at least one or the client or server, to function in a specified manner to provide message communications, the message communications occurring in a computer system hardware architecture neutral and operating system neutral and network transport protocol neutral manner for a resource owner authorizing a specific user the right to access a particular resource, the program module including instructions for:

A. sending a resource tag to a specified user;

B. receiving, back from the specified user, the resource tag sent earlier and a user credential information;

C. verifying the user credential information;

D. comparing a first cryptographic transformation of a first information item to a second cryptographic transformation of a second information item; and

E. granting access to the particular resource only if the first cryptographic transformation of the first information item has a predetermined relationship with the second cryptographic transformation of the second information items, and otherwise denying access to the particular resource.

2. A hardware architecture neutral and operating system neutral and network transport neutral method for a resource owner authorizing a specific user the right to access a particular resource, said method comprising:

A. sending a first information item to a specified user;

B. receiving, back from the specified user, the resource tag sent earlier and a user second information item;

C. verifying the user second information item; and

D. comparing a first cryptographic transformation of the first information item to a second cryptographic transformation of the second information item; and

E. granting access to the particular resource only if the first cryptographic transformation of the first information item has a predetermined relationship with the second cryptographic transformation of the second information items, and otherwise denying access to the particular resource.

3. The method in claim 2, wherein said particular resource comprises an e-mail message.

4. The method in claim 2, wherein said particular resource comprises a promotional coupon.

5. The method in claim 2, wherein said particular resource comprises an information item in electronic form.

6. The method in claim 2, wherein said particular resource comprises a storymail story.

7. The method in claim 2, wherein the resource tag comprises a message tag or a coupon tag.

8. The method in claim 2, wherein the resource tag is generated as the result of a reversible cryptographic transformation.

9. The method in claim 2, wherein the first information item comprises a redundancy field and the second information item comprises a resource identifier field and said transformation comprises a transformation of one or more of the Redundancy Field and the Resource Identifier Field.

10. The method in claim 9, wherein at least one of the redundancy field and resource identifier field include a message number.

11. The method in claim 2, wherein said transformation comprises a transformation of a Redundancy Field, a Resource Identifier Field, and other information.

12. The method in claim 2, wherein the resource tag comprises a message tag or a coupon tag and is generated as the result of a reversible cryptographic transformation, the transformation comprising a transformation of at least a Redundancy Field and a Resource Identifier Field, at least one of the redundancy field and resource identifier field including a message number.

13. The method in claim 2, wherein said resource tag is sent by any one of conventional e-mail, Story Enabled e-mail, display on a web page, or hardcopy media.

14. The method in claim 12, wherein the fields of a Resource Tag are based on one or more secret keys known to the Resource Owner.

15. The method in claim 14, wherein the one or more secret keys known to the resource owner use one or a series of block encryption steps on portions of the fields in a manner that allows the transformation to be reversed by an entity that knows the one or more secret keys.

16. The method in claim 15, wherein the resource tag comprises a nine-byte to sixteen-byte tag, and the cryptographic transformation is performed by three or more applications of eight-byte block encryption using a cipher.

17. The method in claim 16, wherein a portion of the output bits from each of the applications of eight-byte block encryption are exclusively OR'ed with a portion of the input bits to the next one of the applications of eight-block encryption.

18. The method in claim 16, wherein said cipher is selected from the group of ciphers consisting of a triple-DES based cipher, a XTEA based cipher, a RC5 based cipher, and combinations thereof.

19. The method in claim 15, wherein the resource tag has an arbitrary length and the cryptographic transformation is performed by a block cipher.

20. The method in claim 19, wherein said block cipher is operating in Cipher-Block-Chaining mode.

21. The method in claim 20, wherein said Cipher-Block-Chaining mode operates with an initialization vector.and said initialization vector has a fixed value.

22. The method in claim 21, wherein said initialization vector is applied in two passes, a first pass in a first direction (from left to right) across the bytes of the fields and then a second pass in the opposite direction to the first pass (from right to left) across those resulting bytes, with the end result being that of generating resource tag bits which together form said resource tag, and wherein each resource tag bit depends strongly on bits of the input fields, so that only an entity who knows the one or more keys can reverse this cryptographic transformation.

23. The method in claim 12, wherein the Redundancy Field comprises a cryptographic hash.

24. The method in claim 23, wherein said redundancy field cryptographic hash comprises SHA1 of (i) some or all of a User Credential, and (ii) one or more parts of a Server Credentials.

25. The method in claim 24, wherein said redundancy field cryptographic hash further comprises SHA1 of (iii) one or more other of the optional other input fields of the Resource Tag.

26. The method in claim 25, wherein the optional fields from the Resource Tag include the Resource Identifier.

27. The method in claim 24, wherein the User's Credential includes that user's e-mail address.

28. The method in claim 24, wherein the User's Credential includes an attribute identifying a user or an information appliance, computer, or network interface card address, associated with the user.

29. The method in claim 24, wherein the Server's Credential includes either one or both of the server's internet domain name, or the domain name associated with the Resource Owner.

30. The method in claim 24, wherein the User's Credential includes an attribute identifying a user, a user's e-mail address, or an information appliance associated with the user or email address; and the Server's Credential includes either one or both of the server's internet domain name or the domain name associated with the Resource Owner.

31. The method in claim 2, wherein the verification of the User's Credential is based on a challenge-response authentication protocol.

32. The method in claim 31, wherein the challenge-response authentication protocol is a protocol that proves that the User (client) communicating with the Resource Owner (server) has current access to a private key associated with a public key.

33. The method in claim 32, wherein the private key comprises a RSA private key, an Elliptic Curve private key, or a NTRU private key.

34. The method in claim 32, wherein the public key appears as one field of the User Credential Information.

35. The method in claim 34, wherein the User Credential Information is digitally signed along with other credential information by an entity that is trusted by the Resource Owner.

36. The method in claim 31, wherein the challenge-response protocol indicates that the User (client) communicating with the Resource Owner (server) has current access to a secret key associated with a key identifier.

37. The method in claim 36, wherein the secret key comprises a triple-DES based secret key, a XTEA based secret key, a RC5 based secret key, or a AES based secret key.

38. The method in claim 36, wherein the key identifier appears as one field of the User Credential information.

39. The method in claim 36, wherein the key identifier allows the server to look up the same secret key known to the client.

40. The method in claim 38, wherein the key identifier allows the server to look up the same secret key known to the client, and other fields in the User Credential Information are verified using a cryptographic checksum based on that same secret key.

41. The method in claim 2, wherein the first information comprises the Resource Tag, and the second information item comprises some portion or all of the User Credential Information and one or more portions of the Server's or Resource Owner's Credential Information.

42. The method in claim 41, wherein said second information item optionally comprises one or more of the input fields to the Resource Tag.

43. The method in claim 2, wherein said comparison comprises a logical operation.

44. The method in claim 43, wherein said comparison comprises a logical operation performed on a bit, byte, multi-bit, or multi-byte basis.

45. The method in claim 2, wherein said comparison comprises an algorithm based comparison operation.

46. The method in claim 2, wherein said comparison comprises a mathematical operation.

47. The method in claim 2, wherein the first information comprises the Resource Tag, and the second information item comprises some portion or all of the User Credential Information and one or more portions of the Server's or Resource Owner's Credential Information, and said comparison comprises at least one of a logical operation and a mathematical operation.

48. The method in claim 2, wherein said predetermined relationship is equality.

49. The method in claim 2, wherein said comparison comprises at least one of a logical operation and a mathematical operation and said predetermined relationship is equality.

50. The method in claim 2, wherein the first information item comprises a redundancy field and the second information item comprises a resource identifier field; and the first cryptographic transformation comprises a process that is the reverse of the process applied to create the resource tag from its input fields followed by an operation that extracts the Redundancy Field.

51. The method in claim 50, wherein the second cryptographic transformation includes substantially the same steps used to create the Redundancy Field based on at least one of the verified User Credential Information and the Server Credential Information.

52. The method in claim 50, wherein the second cryptographic transformation includes substantially the same steps used to create the Redundancy Field based on at least one of the verified User Credential Information and the Server Credential Information, and one or more of the input fields to the Resource Tag.

53. The method of claim 35, wherein the trusted entity comprises a Compact Certificate as explained earlier, or chain of Compact Certificates leading to a trusted root public key.

54. A method for authorizing a user access a resource, said method comprising:

sending a resource tag to the user;

receiving the resource tag and a user credential information from the user;

verifying the user credential information;

comparing a first cryptographic transformation of the resource tag to a second cryptographic transformation of some portion or all of the User Credential Information and one or more selected portions of the Server's or Resource Owner's Credential Information; and

granting access to the resource only if the first cryptographic transformation of the resource tag matches with the second cryptographic transformation of the selected portion or all of the User Credential Information and one or more portions of the Server's or Resource Owner's Credential Information, and otherwise denying access to the resource.